Congress of the United States
Washington, DC 20515

June 5, 2018

The Honorable Alex Azar
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Secretary Azar:

We write to raise concerns regarding the Department of Health and Human Services' (HHS) implementation of Section 405 of the Cybersecurity Information Sharing Act of 2015 (CISA). Specifically, we request information regarding the "Cyber Threat Preparedness Report" (CTPR) required by 405(b) of the Act, as well as a status update regarding the alignment of "Health Care Industry Security Approaches" required by 405(d), and urge HHS to take prompt actions to address these outstanding issues. As cyber threats to the health care sector increase in frequency and severity, it is imperative that HHS provide clear and consistent leadership and direction to the sector regarding cyber threats.

On April 27, 2017, HHS delivered the CTPR to the House Committee on Energy and Commerce and the Senate Committee on Health, Education, Labor & Pensions (collectively, the Committees).[1] This report was intended to clarify HHS's internal roles, responsibilities, and preparedness to address cyber threats in the health care sector.[2] Since the preparation and delivery of the CTPR, however, HHS has continued to alter its cybersecurity strategy.

While the CTPR provided a high-level overview of the cybersecurity responsibilities of each HHS office and operating division, the report omitted or lacked sufficient detail on many outstanding issues. For example, HHS is both a regulator of the health care sector and the Sector Specific Agency (SSA) responsible for leading and providing guidance under the national critical infrastructure protection model. HHS must make clear how it plans to carry out this dual role and clearly communicate to stakeholders, who must balance the need for support from HHS during cybersecurity incidents with the perceived risk that seeking support could lead to regulatory enforcement actions. The CTPR did not mention this dual role or provide any clarification as to when HHS will act as a regulator or an SSA and how it will transition from one role to the other.

[1] *HHS Cyber Threat Preparedness Report*, DEP'T OF HEALTH AND HUMAN SERV. (2017) (hereafter *CTPR*). The CTPR is on file with both Committees.

[2] Consolidated Appropriations Act, 2016, Pub. L. 114-113, 129 STAT. 2981-2984, 18 Dec. 2015, https://www.gpo.gov/fdsys/pkg/PLAW-114publ113/pdf/PLAW-114publ113.pdf (hereafter *CISA 2015*). The Cybersecurity Information Sharing Act of 2015 was passed as part of the larger bill, with the health care cybersecurity portions contained in Section 405.

Similarly, the CTPR failed to document HHS's policies and procedures for responding to cybersecurity concerns or incidents that implicate multiple HHS operating divisions or offices. For example, a cybersecurity incident may initially affect a health care provider's electronic health records, requiring a response from the Office of Civil Rights or the Office of the National Coordinator. If such an incident also compromised medical devices, the Food and Drug Administration likely would need to respond as well. The CTPR did not provide additional details or clarification as to how HHS would handle such an incident, when it would be appropriate for one HHS operating division or office to share information with another, or how such sharing would occur. This policy gap creates confusion for stakeholders and complicates the already difficult task of responding to cybersecurity incidents.

Most notably, the CTPR lacked information regarding the Healthcare Cybersecurity and Communications Integration Center (HCCIC). The HCCIC was announced during a panel appearance in April 2017 by the then-HHS Chief Information Security Officer, who stated, "HHS is building a health care information collaboration and analysis center, just like the [Department of Homeland Security's] NCCIC, only focused on health care."[3] Few additional details were provided, offering little clarity on how the HCCIC would fit into the larger health care cybersecurity picture and raising concerns that the HCCIC could duplicate work by entities such as the NCCIC or National Health-Information Sharing and Analysis Center (NH-ISAC).[4] Now a year after the announcement, the clearest public information regarding the HCCIC comes from written testimony submitted by HHS to the Energy and Commerce Committee for a June 2017 hearing.[5]

That testimony stated:

> "HHS supports the [Healthcare and Public Health] sector through the establishment and operation of the [HCCIC]. The HCCIC has three high level goals:
>
> - Strengthen engagement across HHS Operating Divisions;
> - Strengthen reporting and increase awareness of the health care cyber threats across the HHS enterprise; and
> - Enhance public-private partnerships through regular engagement and outreach."[6]

[3] Nicole Ogrysko, *HHS to stand up its own version of the NCCIC for health*, FEDERAL NEWS RADIO (Apr. 20, 2017), https://federalnewsradio.com/health-it/2017/04/hhs-to-stand-up-its-own-version-of-the-nccic-for-health/.

[4] Letter from the Hon. Ron Johnson and the Hon. Claire McCaskill, S. Comm. On Homeland Sec. and Gov't Affairs, to the Hon. Tom Price, Sec'y, US. Dep't of Health and Human Serv. (June 21, 2017).

[5] *Testimony from Emery Csulak, Steven Curren, and Leo Scanlon on Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity before Committee on Energy and Commerce,* U.S. DEP'T OF HEALTH AND HUMAN SERV. (June 8, 2017), https://www.hhs.gov/about/agencies/asl/testimony/2017-06/examining-role-department-health-and-human-services.html.

[6] *Id.*

If HHS envisions the HCCIC as a mechanism to fulfill many of its cybersecurity goals and responsibilities, including those that HHS already assigned to various divisions and subdivisions, it is unclear why HHS omitted the HCCIC from the CTPR. The HCCIC was announced in April 2017 with the intention that it would be operational by June 2017. The absence of the HCCIC within the CTPR in May of 2017 renders the report outdated, incomplete, and inaccurate.

Further, there is significant confusion regarding the role and status of the HCCIC:

1. The global health care sector suffered a massive ransomware outbreak known as WannaCry in May 2017, which posed such a severe threat to the United States health care sector that HHS activated the HCCIC a month early.[7] The United States was ultimately spared the damage suffered by other countries, which media reports have attributed to the timely intervention of an unaffiliated security researcher, rather than specific actions taken by HHS or health care stakeholders.[8] HHS nonetheless credits the HCCIC and the capabilities it enabled for the relatively smooth sector response to the crisis.[9]

2. In September 2017, HHS temporarily reassigned two senior officials responsible for the day-to-day operation of the HCCIC to unrelated duties.[10] Memoranda provided to the affected officials stated the reassignments were to "permit the Agency time to review allegations raised against the Office of the Chief Information Officer (OCIO), Office of Information Security."[11] HHS's removal of senior HCCIC personnel has had undeniable impacts on HCCIC and HHS's cybersecurity capabilities.

Stakeholders have informed our staffs that they no longer understand whether the HCCIC still exists, who is running it, or what capabilities and responsibilities it has. Responses to committee requests to HHS for clarification on these questions remain vague at best, and the lack of documentation provided continues to undermine HHS's efforts to address the HCCIC's status.[12]

Further, HHS's private and public representation of the HCCIC as central to its cybersecurity efforts has confounded efforts to understand how HHS meets its obligations related to cybersecurity given the HCCIC's instability. The HCCIC's surprise announcement, initial

[7] Lily Hay Newman, *The Ransomware Meltdown Experts Warned About is Here*, WIRED, Mar. 12, 2017, https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.

[8] Lily Hay Newman, *How An Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack*, WIRED, May 13, 2017, https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/.

[9] *Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity: Hearing Before the H. Comm. on Energy and Commerce,* 115th Cong. (June 8, 2017), http://docs.house.gov/meetings/IF/IF02/20170608/106078/HHRG-115-IF02-Transcript-20170608.pdf (*See* statements from Steve Curren and Leo Scanlon regarding HCCIC and the WannaCry outbreak).

[10] Letter from the Hon. Greg Walden, Hon. Frank Pallone, Jr., and Hon. Diana DeGette, H. Comm. on Energy and Commerce, to Eric Hargan, Acting Sec'y, Dep't of Health and Human Serv. (Nov. 14, 2017), https://energycommerce.house.gov/wp-content/uploads/2017/11/20171114HHS.pdf.

[11] *Id.* at 1.

[12] Briefings with Committee staff.

success, and subsequent troubles, combined with the inadequacies in the CTPR, have exacerbated the very issues that CISA was intended to address. HHS's decision to present to our Committees a report that was outdated, incomplete, and inaccurate raises concerns about HHS's ability to address the growing number and severity of cyber threats facing the health care sector.

Additionally, 405(d) of CISA required HHS to establish a "collaborative process" with other government officials and health care industry stakeholders to align and publish "Health Care Industry Security Approaches." CISA was signed into law on December 18, 2015, but as of this writing, HHS still has not produced the "common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes" required by the law.

Therefore, we respectfully suggest that HHS take the following actions:

1. Update the CTPR to include any and all changes, modifications, and evolutions that have occurred in HHS cybersecurity strategies since its original drafting.

2. Include within the updated CTPR a detailed explanation of the HCCIC, its roles and responsibilities, how its work and operations intersect with the NCCIC and the NH-ISAC, and how it fits into HHS's broader cybersecurity capabilities and responsibilities.

3. Add sections to the CTPR specifically addressing:

    a. The internal coordination between HHS offices and operating divisions that have regulatory authority with regards to health care cybersecurity, and how those offices will coordinate their efforts to provide a "whole-of-department" response to modern cybersecurity challenges;

    b. The role of HHS, including the responsibility of HHS offices and operating divisions, in securing its own internal information systems as compared to its role in providing guidance, information, education, training, and assistance to the health care sector, and how it will differentiate between those two roles; and

    c. The challenges HHS faces as both the regulator and the Sector Specific Agency for health care, including how it will differentiate and transition between these two roles.

4. Provide the date you expect to release the alignment of "Health Care Industry Security Approaches" required by 405(d) of CISA.

We appreciate your prompt attention to these suggested actions and request that HHS respond by no later than June 19, 2018. We look forward to working with you constructively to improve HHS cybersecurity efforts. If you have any questions regarding this request, please contact Jessica Wilkerson or Alan Slobodin of the House Committee on Energy and Commerce Majority staff at (202) 225-2927, Julie Babayan or Kevin McAloon of the House Committee on Energy and Commerce Minority staff at (202) 226-3400, Bobby McMillin of the Senate

Committee on Health, Education, Labor, and Pensions Majority staff at (202) 224-1284, and Elizabeth Letter of the Senate Committee on Health, Education, Labor, and Pensions Minority staff at (202) 224-0767.

Sincerely,

Greg Walden

Greg Walden
Chairman
Committee on Energy and Commerce
U.S. House of Representatives

Lamar Alexander

Lamar Alexander
Chairman
Committee on Health, Education, Labor,
and Pensions
U.S. Senate

Frank Pallone, Jr.

Frank Pallone Jr.
Ranking Member
Committee on Energy and Commerce
U.S. House of Representatives

Patty Murray

Patty Murray
Ranking Member
Committee on Health, Education, Labor,
and Pensions
U.S. Senate